Rethinking Cybersecurity for Distributed Science

Deb Agarwal
DAAgarwal@lbl.gov
Lawrence Berkeley Laboratory

Threats

- Viruses
- Worms
- Malicious software downloads
- Spyware
- Stolen credentials
- Insider Threat
- Denial of service
- Root kits
- Session hijacking
- Agent hijacking
- Man-in-the-middle
- Network spoofing
- Back doors
- Exploitation of buffer overflows and other software flaws
- Phishing
- Audits / Policy / Compliance
- ?????

Threats

- Viruses
- Worms
- Malicious software downloads
- Spyware
- Stolen credentials
- Insider Threat
- Denial of service
- Root kits
- Session hijacking
- Agent hijacking
- Man-in-the-middle
- Network spoofing
- Back doors
- Exploitation of buffer overflows and other software flaws
- Phishing
- Audits / Policy / Compliance
- ?????

Example - Credential Theft

- Widespread compromises
  - Over 20++ sites
  - Over 3000+ computers
  - Unknown # of accounts
  - Very similar to unresolved compromises from 2003
- Common Modus Operandi
  - Acquire legitimate username/password via keyboard sniffers and/or trojaned clients and servers
  - Log into system as legitimate user and do reconnaissance
  - Use “off the shelf” rootkits to acquire root
  - Install sniffers and compromise services, modify ssh-keys
  - Leverage data gathered to move to next system
- ***The largest compromises in recent memory (in terms of # hosts and sites)***

Cybersecurity Trend - Reactive

- Firewall everything – only allow through vetted applications with strong business need
- Users never have administrator privileges
- All software installed by administrators
- ***All systems running automated central configuration management and central protection management***
- ***Background checks for ALL government employees, contractors, and users with physical presence for issuance of HSPD-12 cards (PIV)***
- ***No access from untrusted networks***
- ***Conformance and compliance driven***
- ***It is a war***

Distributed Science Reality

- Collaborations include as many as 1000's of scientists
- Collaborators located all over the world
- Many users never visit the site
- Virtual organization involved in managing the resources
  - Include multiple sites and countries
  - Distributed data storage
  - Distributed compute resources
  - Shared resources
- Do not control the computers users are accessing resources from
- High performance computing, networking, and data transfers are core capabilities needed
- Authentication, authorization, accounting, monitoring, logging, resource management, etc built into middleware
- ***These new science paradigms rely on robust secure high-performance distributed science infrastructure***

Virtual Organization (VO)

- Includes multiple real organizations/sites and stakeholders
- Supporting users spread around the globe
- Needs to be able to coordinate resource utilization
- Issues
  - Contain impact of a compromised user and host credentials
  - Minimize impact of compromise of services
  - Response to and control of incidents tested in realistic distributed environments
  - Latency of response to and containment of incidents minimized.
  - Usable and timely forensic information
  - Stakeholders (site security, VO administration, etc) need to be able to monitor and control local security and coordinate with the VO

Current Operational Reality

- Cybersecurity group
  - Protect border
  - Protect network
  - Some host protections
  - Control access patterns
- System Administrators
  - Protect hosts
  - Authorize users
  - Define access capabilities
- Applications and software
  - Authenticate users
  - Authorize users
  - Open ports/connect to servers/transfer data
- Virtual Organizations
  - Fine-grained authorization
  - Policy enforcement

Cybersecurity and Infrastructure to Support Distributed Science

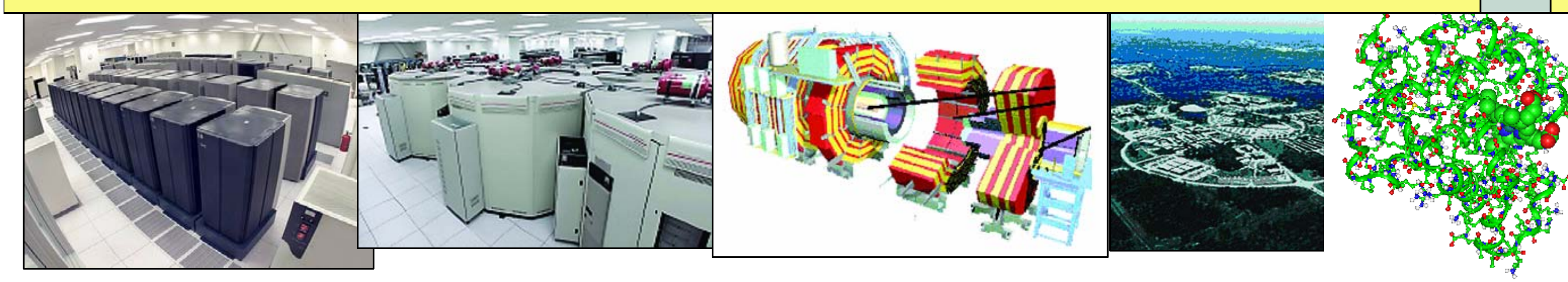
- Preserve
  - Access to national user facilities
  - Participation in international collaborations
  - Ability to host scientific databases and repositories
  - Innovation and prototyping capabilities
- Protect
  - High performance computers
  - Experiment systems
  - Desktop and laptop systems
  - Ability to do science
- ***Need to figure out how to preserve and support open science while protecting the resources from cyber incidents***

Robust Science Support Framework

Web Services, Portals, Collaboration Tools, Problem Solving Environments

- Authentication and Authorization
- Resource Discovery
- Secure Communication
- Event Services And Monitoring
- Data Transfer
- Scheduling
- Data Curation
- Compute Services
- Application Servers
- Asynchrony Support
- Virtual Organization

Cybersecurity Protections



Science is on the Front Lines

- The techniques needed to protect the open science environment today are needed by other environments tomorrow – Past examples
  - Network intrusion detection
  - Insider threat
  - Defense in depth
  - High performance capabilities
- A next set of concerns
  - Reducing credential theft opportunities
  - Detection of insider attacks
  - Communication and coordination between components to recognize and react to attacks in real time
  - Tools which address day zero-1 vulnerabilities
  - Improved analysis techniques – data mining and semantic level searches
  - Prevention and detection of session hi-jacking

HEP Cybersecurity Workshop – March 2005

- Identified a number of critical areas to be addressed
- Vulnerabilities to a potential incident
  - Loss of unique data
  - Insertion of fraudulent data
  - Inability to reestablish control of the computing infrastructure after an incident.
  - Subversion of system software (loss of integrity)
  - Inability to ingest detector output
  - Massive coherent failure of the ensemble of resources
  - Compromise of key infrastructure
  - Pervasive slow down due to compromise that couldn’t be removed

Enabling Virtual Organizations (HEP Workshop)

- Real-time Security Logging and Auditing Service
- Auditing of all necessary components integrated with information service
- Resource vulnerability scanning coordinated with sites
- Intrusion Detection Systems / Intrusion Prevention Systems deployment
- Border Control (site and VO)
- Cybersecurity mechanisms configuration verification

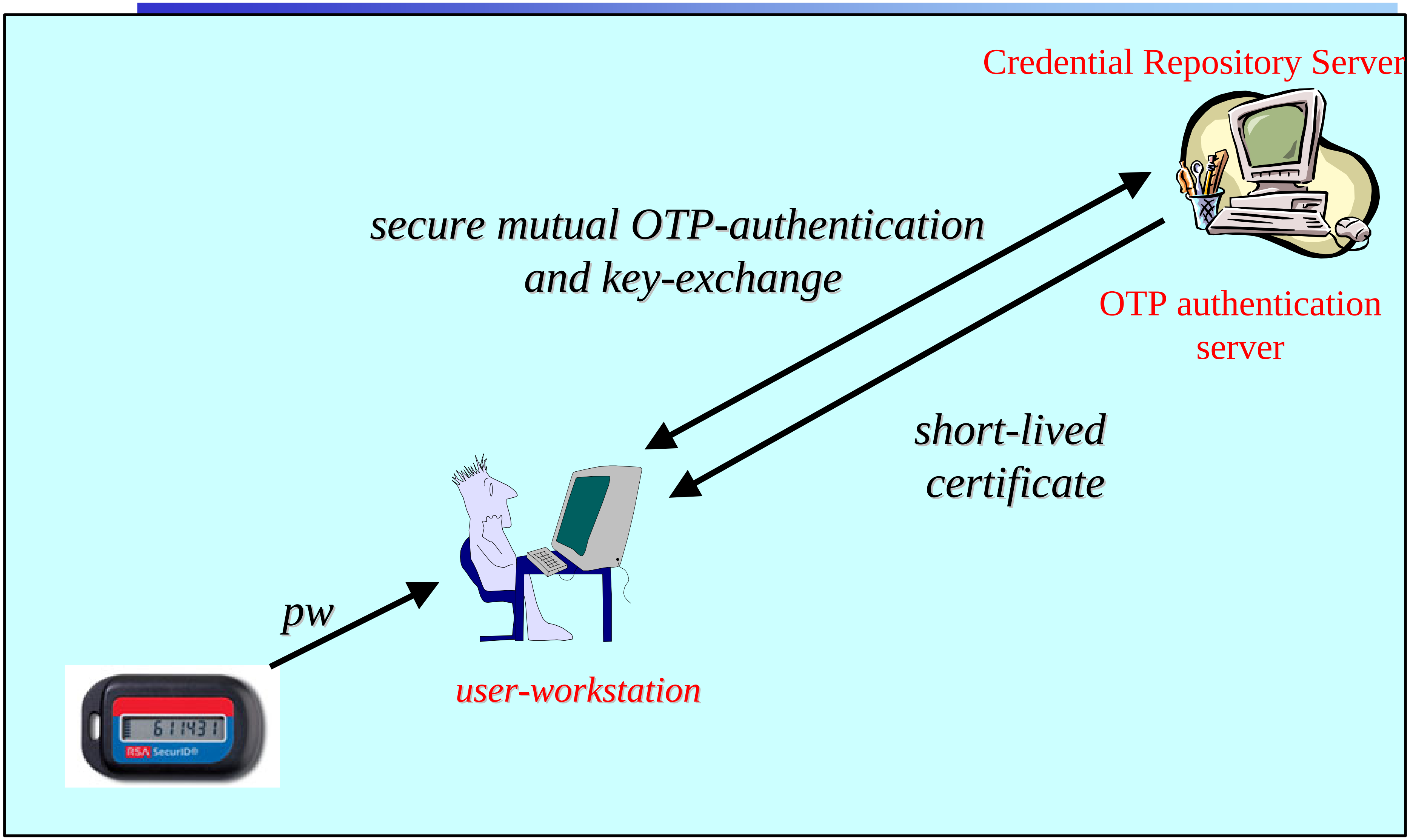
HEP Proposed Program of Work

- Risk analysis and best practices
- Security logging and auditing service
- Incident response and recovery (coordinated across the VO and sites)
- Middleware vulnerability testing and analysis
- Other work
  - Wide-Area Network Monitoring
  - Data Integrity
  - Authentication / Authorization Issues
  - Authorized Audit Log Write/Read Access
  - Disposable Execution Environments
  - Rootkit detection

Proposed Cybersecurity R&D Program

- Coordination of distributed science software infrastructure with cybersecurity mechanisms
  - Authentication, authorization, and encryption in the middleware can coordinate with the cybersecurity systems to open temporary ports etc
- Coordination between cybersecurity components
  - Significantly improve detection of attacks; particularly insider attacks
  - Notify broadly of attacks as they are identified
  - Improve handling of encrypted sessions
- Improved risk- and mission-based cybersecurity decisions
- New authentication, credential translation, and proxy mechanisms
- Data integrity protection/recovery
- Tools for the high-performance computing environment
  - Analysis tools which can efficiently ingest and analyze large quantities of data
  - Semantic level investigation of data
  - Security tools for high bandwidth reserved paths
- Improved data collection, forensics, recovery
- ***Focus on practical solutions, integrating middleware security, and working with operations personnel during the design, development, and testing***

Using OPKeyX in Grid environments



Conclusions

- Distributed science has become core to the conduct of science
- Robust, **secure**, and supported distributed science infrastructure is needed
- Attackers are getting more malicious and quicker to exploit vulnerabilities
- Distributed science requires a fresh approach to cybersecurity
- Need to set the example for protecting distributed infrastructure
- COTS is a key component of the solution but will not solve many aspects of the problem
- ***Need to partner cybersecurity operations, cybersecurity researchers, system administrators, and middleware developers***